Consultation feedback on draft Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data as proposed by the EDPB[1]

Topic	Section	Comment
Step 3 - Assess the law or practice of the third country to ensure the transfer tool is effective	2.3	We noticed that reference has been made to 1) other recommendations from the EDPB to assess the legal framework governing access by public authorities in a third country and 2) the legal context of the transfer as criteria to assess the level of protection of third country regulations. Nevertheless, it seems to us that the CJEU judgment Schrems II requires a more comprehensive case-by-case risk evaluation for each international data transfer - instead of the investigation suggested by the EDPB which would eventually apply to the whole group of transfers going to the same third country. The EDPB guidelines don't encompass this risk assessment however which covers risk factors that are linked to the transferred data, besides the legal context and national legal framework. Could the EDPB clarify whether the circumstances listed in section 2.3 and the referred recommendations are exhaustive? Or should companies also take into account risk factors such as[2]: ○ Nature of the data, differentiating between content and metadata; ○ Volume of data, incl. number of data subjects; ○ Transfer purpose (fraud prevention, advertising etc.); ○ Nature of the transfer (intragroup, controller – to – processor etc.); ○ Duration and frequency of the transfer; ○ Applicable retention period; ○ Impact of transfer on different categories of data subjects; ○ Technical controls and organizational measures in place;

[1] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

[2] CIPL mentions several risk factors in its whitepaper *'A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision'*: https://www.informationpolicycentre.com/cipl-white-papers.html

		○ Risk vetting of processors and sub-processors involved; ○ Other elements listed in the draft SCC Annex, section II, clause 2(b) from the EC;
Use Case 6 - Access to data by cloud services providers	p. 26	Could the EDPB clarify whether its conclusion of the non-availability of technical measures would also apply to pseudonymized data, i.e. the scenario in which the cloud service provider would have access to personal data without direct information related to the identity of the data subject? Would such event still be considered to fall under the scenario described in Use Case 2? More in general: which use case scenario would apply when there's a conflict because an event could fall under multiple use case scenarios? Could the EDPB further clarify whether the outcome of the risk assessment on the nature of the transfer could change its opinion regarding Use Case 6?
Use Case 7 - Remote access to data for business purposes	p. 27	We understand that the data importer will have access to data that directly identifies the data subject within the context of business purposes as the data importer will provide a service on behalf of the data exporter directly to the data subject. Could the EDPB clarify whether its conclusion of the non-availability of technical measures would also apply to pseudonymized data, e.g. the data importer receives pseudonymized data from the data exporter and is not able to link that information directly to the identity of the data subjects? Could the EDPB further clarify what the outcome would be in a use case of remote access within the scope of a global support model for B2B services where the data importer / service provider will have access to pseudonymized data though never communicate directly with customers of its business client, but only with the business client?